REMARKS

The non-final Office Action dated October 16, 2008 was received and carefully reviewed.

By this response, claims 1 and 24 are hereby amended to clarify the invention, and not for reasons of patentability. No claims have been canceled, and no claims have been amended. Thus, claims 1-26 remain pending in the instant application.

Applicant respectfully requests reconsideration and allowance of the above-identified application in view of the above amendments and the following remarks.

Rejections under 35 U.S.C. § 101

Claims 1-14 and 24-26 stand rejected under 35 U.S.C. § 101 because the claimed invention is allegedly directed to non-statutory subject matter. Applicants traverse this rejection for at least the following reasons.

The amendment to claims 1 and 24 obviate any perceived issue of statutory subject matter in the claims, which noted by the Examiner. Accordingly, Applicant respectfully requests the withdrawal of this rejection.

Rejections under 35 U.S.C. § 112

Claims 8-10 and 21 stand rejected under 35 U.S.C. § 112, second paragraph, as allegedly being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. Applicant traverses this rejection for at least the following reasons.

Applicant respectfully submits that information related assets are by definition "a useful material that may contain, manipulate and/or generate information." This definition is in accordance with International Standards ISO/IEC 27001 Information Security Management System (ISMS) where information related assets are defined as being at least one of "information, software, physical, service, people and intangible."

Accordingly, Applicant contends that the assets being "information related" is not indefinite, for at least the reasons stated above. Thus, Applicant respectfully requests the withdrawal of this rejection.

Rejections under 35 U.S.C. § 103

Claims 1, 6, 8, 14, 16, 19, 21 and 23-26 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Tschiegg et al. (U.S. Pat. Pub. No.: 2003/0160818 A1) (*Tschiegg*, hereinafter) in view of Heinrich (U.S. Pat. Pub. No.: 2003/0046128 A1) (*Heinrich*, hereinafter). Claims 2-5, 7, 9-13, 15, 20 and 22 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over *Tschiegg* in view of *Heinrich* and in further view of Lovejoy et al. (U.S. Pat. Pub. No.: 2002/01238416 A1) (*Lovejoy*, hereinafter). Applicant traverses these rejections as follows.

Applicant contends that present independent claims 1 and 16, and the claims dependent therefrom, are patently distinguishable over *Tschiegg*, *Heinrich* and *Lovejoy*, since *Tschiegg* and *Heinrich* and *Lovejoy*, taken either alone or in combination, fail to disclose, teach or suggest all of the features recited in the pending claims. For example, independent claim 1 (emphasis added) recites:

> A computer-implemented method for assessing risk within an organization, comprising:
>
> defining one or more zones, each of said one or more zones comprising an environment;
>
> identifying one or more assets of said organization, each of said assets being located in a respective one of said zones;
>
> **conducting a respective impact assessment for each of said assets, each assessment comprising assessing the impact of the loss of said respective asset;**
>
> **conducting for each of said zones a respective zone risk assessment, comprising assessing the risk level associated with placing a respective asset within said respective corresponding zone;**
>
> **conducting for each asset a respective asset risk assessment, comprising assessing the risk level associated with said respective asset independent of the respective zone of said respective asset**; and
>
> assessing risk on the basis of at least said impact assessment, said zone risk assessments and said asset risk assessments.

Independent claim 16 (emphasis added) recites:

> An apparatus for assessing risk within an organization, comprising:
>
> data input means for inputting asset information into a register of assets, each of said assets being an asset of said organization, each of said assets being located in a respective zone;
>
> data storage for storing said register of assets, including for each of said assets said respective zone;
>
> means for receiving or storing a respective zone risk assessment for each of said zones, said respective zone risk assessment comprising an assessment of the risk level associated with placing a

> respective asset within said respective corresponding zone;
>
> means for receiving or storing a respective asset risk assessment for each asset, said respective asset risk assessment comprising an assessment of the risk level associated with said respective asset independent of the respective zone of said respective asset;
>
> means for receiving or storing a respective impact assessment for each of said assets, each assessment comprising assessing the impact of the loss of said respective asset, and for assessing risk on the basis of at least said impact assessment, said zone risk assessments and said asset risk assessments to thereby form a risk assessment; and
>
> output means for outputting said risk assessment.

Thus, independent claims 1 and 16 are directed to, *inter alia*, the features conducting a respective impact assessment for each of said assets, each assessment comprising assessing the impact of the loss of said respective asset, conducting for each of said zones a respective zone risk assessment, comprising assessing the risk level associated with placing a respective asset within said respective corresponding zone, conducting for each asset a respective asset risk assessment, comprising assessing the risk level associated with said respective asset independent of the respective zone of said respective asset. Applicants contend that *Tschiegg*, *Heinrich* and *Lovejoy*, taken either alone or in combination, fail to disclose at least the above recited features of independent claims 1 and 16.

A zone, as defined by the present invention, may be characterized as either "real" or "virtual", i.e., a zone of the present invention may be a physical area, a network or a custodial practice. For example, a network zone may be identified as a DMZ and an internal LAN. A physical zone may be identified as an office area and/or a data center. Further, a custodial practice zone may be identified as Microsoft Windows and Linux administration (see the specification, e.g., pages 20-22). Contrary to the present invention, *Tschiegg* merely discloses that a zone is a physical location, i.e., a property (see *Tschiegg*, e.g., paragraph [0009]). Furthermore, another distinguishing feature of the present invention is that a "zone" may be viewed as a sub-zone where a plurality of "zones" are defined within a property, while the zone concept disclosed in *Tschiegg* is completely silent with regard to any notion that a zone may be comprised of "sub-zones", as in the present invention.

In addition, the present invention identifies the assets which are associated with a zone so that risks can be accounted for. However, the method described in *Tschiegg* is completely silent with regard to this feature of the present invention, but instead is directed to the identification of the risk associated with a property, so that lost assets can be accounted for, which is the opposite of the teachings of the present invention.

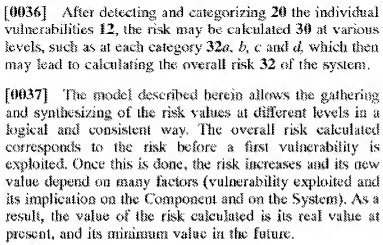
The Examiner has cited paragraph [0019] of *Tschiegg*, as allegedly teaching "determining loss before and after implementation of recommendation" (see, e.g., paragraph 16c. of the Office Action). However, Applicant contends that the claims do not recite *determining loss before and after implementation of recommendation*, as alleged by the Examiner, but rather the claims state "conducting a respective impact assessment for each of said assets, each assessment comprising assessing the impact of the loss of said respective asset".

Applicant further contends that the present invention computes loss based on the potential worst case consequential impacts. The impact criteria of the present invention are as follows: 1) Loss of Opportunity, 2) Loss of Productivity, 3) Loss due to Regulatory and Contractual Breaches, 3) Cost of System Investment, and 4) Loss due to Confidentiality Breaches. Thus, as clearly seen in the list of impact criteria, <u>there is no consideration of risk analysis recommendations</u>. Consequently, the rejection the Examiner's rejection of the claims citing that *Tschiegg* discloses *determining loss before and after implementation of recommendation* is <u>improper</u>.

The Examiner cites paragraphs [0058]-[0069] as allegedly disclosing the feature of "conducting for each of said zones a respective zone risk assessment", as recited in independent claims 1 and 16. However, paragraphs [0058]-[0069] actually recite that the filter function is merely associated with a reporting format, and <u>not</u> with "conducting for each of said zones a respective zone risk assessment", as alleged by the Examiner.

As the Examiner correctly admits, "Tschiegg does not explicitly teach assessing a risk of the asset within a zone", and is reliant upon Heinrich for disclosing this feature.

Specifically, the Examiner cites paragraphs [0036]-[0037] of *Heinrich* as allegedly the disclosing the "assessing the risk level associated with an asset" and "assessing the risk level associated with said respective asset independent of the respective zone of said respective asset" feature of present independent claims 1 and 16. However, paragraphs [0036]-[0037] of *Heinrich* actually recite:



> **[0036]** After detecting and categorizing **20** the individual vulnerabilities **12**, the risk may be calculated **30** at various levels, such as at each category **32***a*, *b*, c and *d*, which then may lead to calculating the overall risk **32** of the system.
>
> **[0037]** The model described herein allows the gathering and synthesizing of the risk values at different levels in a logical and consistent way. The overall risk calculated corresponds to the risk before a first vulnerability is exploited. Once this is done, the risk increases and its new value depend on many factors (vulnerability exploited and its implication on the Component and on the System). As a result, the value of the risk calculated is its real value at present, and its minimum value in the future.

Thus, as seen above *Heinrich* fails to disclose "assessing the risk level associated with an asset" and/or "assessing the risk level associated with said respective asset independent of the respective zone of said respective asset". Moreover, *Heinrich* merely describes the risks associated with risks associated with hackers finding vulnerabilities in various components of a computer system (see *Heinrich*, e.g., paragraph [0053]-[0054]), and is <u>completely silent</u> with regard to assets of any kind. Consequently, *Heinrich* cannot disclose "assessing the risk level associated with an <u>asset</u>" and "assessing the risk level associated with said respective asset independent of the respective zone of said respective <u>asset</u>", as recited in independent claims 1 and 16.

Furthermore, applicants respectfully submit that *Lovejoy* fails to make up for the deficiencies of *Tschiegg* and *Heinrich.*

Thus, for at least the reasons stated above both *Tschiegg*, *Heinrich* and *Lovejoy*, taken either alone or in combination, fail to disclose, teach or suggest all of the claimed features of present independent claims 1 and 16. Thus, the Examiner has failed to provide a *prima facie* case of obviousness. Accordingly, Applicants respectfully request the withdrawal of the rejection of independent claims 1 and 16 under 35 U.S.C. § 103(a), and the allowance of these claims.

Claims 2-15 and 17-26 are allowable at least by virtue of their dependency from one of the independent claims, but also because they are distinguishable over the prior art.

In view of the foregoing, it is submitted that the present application is in condition for allowance and a notice to that effect is respectfully requested. If, however, the Examiner deems that any issue remains after considering this response, the Examiner is invited to contact the undersigned attorney/agent to expedite the prosecution and engage in a joint effort to work out a mutually satisfactory solution.

Except for issue fees payable under 37 C.F.R. § 1.18, the Commissioner is hereby authorized by this paper to charge any additional fees during the entire pendency of this application including fees due under 37 C.F.R. §§ 1.16 and 1.17 which may be required, including any required extension of time fees, or credit any overpayment to Deposit Account No. 19-2380. This paragraph is intended to be a **CONSTRUCTIVE PETITION FOR EXTENSION OF TIME** in accordance with 37 C.F.R. § 1.136(a)(3).

Respectfully submitted,

NIXON PEABODY, LLP

Date: January 21, 2009

/Anthony J. Canning, Reg. #62,107/
Anthony J. Canning
Registration No. 62,107

NIXON PEABODY LLP
401 9th Street, N.W., Suite 900
Washington, D.C. 20004-2128
(202) 585-8000